TITLE OF THE INVENTION

METHOD, APPARATUS, AND PROGRAM FOR PROCESSING SIGNATURE, AND STORAGE MEDIUM THEREFOR

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to methods, apparatuses, and programs for processing an input handwritten signature in order to determine whether or not the signature is written by an authentic user, and to storage media therefor.

Description of the Related Art

In general, a conventional user authentication method is performed using a user ID and a password. However, users tend to forget their passwords. In such cases, it is necessary to obtain the password based on the user ID in one way or another, and a security hole results. In order not to forget his/her password, the user often uses a word which is easy to remember, e.g., the user's birthday or the name of the user's child, as the password. The use of an easy-to-remember word as the password, itself is a security hole.

In order to prevent these problems, as described in "Method and Apparatus for Authenticating a Handwritten Character String" disclosed in Japanese Patent Laid-Open No.

10-143668 and in Japanese Patent Laid-Open No. 10-171926, a user authentication method (signature authentication method) is proposed in which handwritten data (signature data) is used in place of a password.

Unlike a password, handwritten data includes the characteristics of a person even when another person inputs the same word. As a result, a person other than the authorized user will fail in user authentication. Such characteristics include the shape of the characters, the stroke order of the characters, writing speed, writing rhythm, and the like.

Unlike fingerprints, the degree of freedom in registration contents is high. By registering a word such as a spell, it becomes more difficult for a person other than the user to pose as a registered user. By registering invariable signature data, the user who has registered the signature data can easily be authenticated.

In conventional authentication methods using passwords, it is possible to hide the input password using a symbol such as "*" in order to hide the password from another person who may be able to see the screen. However, in conventional authentication methods using signatures, signature data input by a user is displayed without any alteration while it is being input, and hence, another person can easily discern the input signature. In order to

prevent this problem, handwritten information can be hidden from the user while it is being input. If this is done, however, it becomes difficult for the user to input the same signature data repeatedly.

In authentication methods using passwords, when a user forgets a password, a hint such as "the name of your pet" is given to the user in order to enable the user to recall the password. However, in conventional authentication methods using signatures, it is very difficult to express the shape of a user's signature in a sentence. When the user forgets the registered signature, it is impossible to assist the user in recalling his/her signature.

SUMMARY OF THE INVENTION

Accordingly, it is an object of the present invention to determine, when an input signature is being displayed on a display unit, whether a predetermined condition is satisfied, and when it is determined that the predetermined condition is satisfied, to display the signature on the display unit in a manner that it is difficult for others to discern the signature.

Preferably, the predetermined condition includes the existence of an instruction by a user to display the signature in a manner that it is difficult to discern the

signature.

Preferably, the predetermined condition includes the failure of the user to remember his/her registered signature.

Preferably, when it is determined that the predetermined condition is satisfied, a combination of the color of a display region of the display unit for displaying the signature and the color of the signature, which makes it difficult to discern the signature, is used.

Preferably, when it is determined that the predetermined condition is satisfied, an image pattern is displayed on the display region of the display unit for displaying the signature.

Preferably, when it is determined that the predetermined condition is satisfied, the input signature is displayed in broken lines.

Preferably, when it is determined that the predetermined condition is satisfied, a portion of the input signature is displayed.

Preferably, the portion of the input signature is a portion input within a predetermined time before the current input time.

Preferably, when it is determined that the predetermined condition is satisfied, the input signature is displayed in a flashing manner.

Preferably, the signature includes coordinate data

which is input using a coordinate input unit.

Further objects, features, and advantages of the present invention will become apparent from the following description of the preferred embodiments with reference to the attached drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are incorporated in and constitute a part of the specification, illustrate embodiments of the invention and, together with the description, serve to explain the principles of the invention, in which:

Fig. 1 illustrates the basic operation of a signature authentication apparatus according to an embodiment of the present invention;

Fig. 2 illustrates a dialog box which asks a user whether or not to re-display a registered signature;

Fig. 3 illustrates an example of a display screen when a signature is registered;

Fig. 4 illustrates a case in which the color a background increases the difficulty in determining the signature;

Fig. 5 illustrates a case in which the signature is displayed on a hatched background;

Fig. 6 illustrates a case in which the signature is partially displayed using dotted lines;

Fig. 7 illustrates a case in which the signature is displayed and deleted immediately thereafter;

Fig. 8 is a flowchart showing a process of displaying the signature as illustrated in Fig. 7;

Fig. 9 illustrates a case in which the signature is displayed in a flashing manner;

Fig. 10 is a flowchart showing a process of displaying the signature as illustrated in Fig. 9;

Fig. 11 is a flowchart showing a process of scrambling and displaying the signature; and

Fig. 12 is a block diagram of the internal structure of the signature authentication apparatus.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Fig. 12 is a block diagram of the internal structure of a signature authentication apparatus according to an embodiment of the present invention. Referring to Fig. 12, a central processing unit (CPU) 1201 reads a program such as a signature processing program for performing processes shown in Figs. 1, 8, 10, and 11 or application software from a read only memory (ROM) 1207 or a flash memory 1208 for storing the program. The CPU 1201 uses a work area, i.e., a

random access memory (RAM) 1206, and executes the program. A coordinate input unit 1202 is a digitizer. The coordinate input unit 1202 obtains a signature written by a user as handwritten data and outputs the handwritten data to the CPU 1201. A display unit 1203 displays information such as the input signature. A communication interface 1204 is used to establish a connection with a network for communication with an external unit. A power supply 1205 supplies power to components in the signature authentication apparatus. The RAM 1206 is the work area used when the CPU 1201 executes the program. The ROM 1207 and the flash memory 1208 are storage media which store the programs, such as the signature processing program for performing the processes shown in Figs. 1, 8, 10, and 11 and the application software, and various types of data such as referential signature data dictionary used in authenticating the signature. The programs may be stored beforehand in the storage media. Alternatively, the programs can be supplied from the outside through removable media or network (communication interface), with the CPU 1201 executing the programs. Although the ROM 1207 and the flash memory 1208 are used as the storage media in this embodiment, storage media such as a hard disk, a floppy disk, a CD-ROM, a DVD, and the like can be used.

Fig. 1 illustrates the basic operation of the signature authentication apparatus of the embodiment.

In a signature inputting step 101, coordinates are input by a so-called digitizer (coordinate input unit 1202). Specifically, a user uses a device such as a pen to input a signature on the digitizer, and the digitizer obtains a coordinate data series for the data input on the digitizer. Alternatively, a digitizer capable of further obtaining, during the signature inputting step 101, information such as the writing force and writing speed can be used.

In the normal operation, signature data 103 input in the signature inputting step 101 is output and displayed on the display unit 1203, which is, for example, a liquid crystal display, in a signature displaying step 102.

The digitizer used in the signature inputting step 101 can be combined with the display unit 1203 in which the digitizer is connected to a desktop computer. Also, the digitizer and the display unit 1203 may not be combined with each other. Preferably, when the digitizer and the display 1203 are combined, as in a liquid crystal tablet integrated-type apparatus, the user can directly input the signature as if the user is writing characters with a pen on paper.

Referential signature dictionary data can be registered by converting the input signature data 103 into signature dictionary data 105 in a signature registering step 104, and the signature dictionary data 105 can be stored in a dictionary.

When authenticating the signature, in a signature authenticating step 106, the signature data 103 input in order to authenticate the signature is matched with the signature dictionary data 105 registered in the dictionary, and an authentication result 107 indicating whether or not the authentication was successful is output.

In a signature re-displaying step 108, if the user forgets the signature, the signature dictionary data 105 registered in the dictionary is displayed in response to an instruction from the user. The registered signature dictionary data 105 is scrambled in a display scrambling step 109 so that another person will have difficulty in discerning the signature, and the signature is displayed in the signature displaying step 102.

In normal signature registration or normal signature authentication, in response to a special instruction given by the user, the input signature data 103 is scrambled in the display scrambling step 109 and is displayed in the signature displaying step 102, instead of being directly displayed in the signature displaying step 102.

Fig. 2 illustrates a dialog box which is displayed when activating the signature re-displaying step 108. Since the signature re-displaying step 108 is a very unsecure step in the authentication system, for example, the number of times the signature is re-displayed is recorded, and the signature

can be re-displayed up to three times.

Fig. 3 illustrates the screen which is displayed when the signature registering step 104 is performed. A non-display check box 302 enables the user to choose whether or not he/she wants to use the display scrambling step 109. When the non-display check box 302 is not selected, the input signature data 103 is clearly displayed with the signature data 103 in black on a white background of a signature display portion 301 (black and white are, of course, merely examples). When the non-display check box 302 is selected, as shown in Fig. 3, the signature data 103 is scrambled in the display scrambling step 109 prior to being displayed on the signature display portion 301. For example, the color of the background is changed, and hence, the input signature data 103 is displayed in a manner that it is difficult to discern the signature.

Fig. 11 is a flowchart showing a process of switching between performing and not performing the display scrambling step 109 in response to an instruction given by the user, such as by selecting the non-display check box 302. In step S1101, the process determines whether an instruction to perform the display scrambling step 109 is given by the user. For example, if the non-display check box 302 is selected, and hence, if it is determined that the instruction to perform the display scrambling step 109 is given by the user,

in step S1102, the process switches the display screen so that it becomes difficult for others to discern an input signature. When no instruction is given by the user to perform the display scrambling step 109, the signature is displayed clearly.

Figs. 4 to 10 illustrate examples where the display scrambling step 109 is used when displaying a signature.

Fig. 4 shows an example in which the signature data 103 and the background are displayed using similar colors of similar brightness. For example, the background and the signature portion are displayed in different colors with the same brightness. Alternatively, the background can be gray, and the signature data 103 can be white. Also, a combination of similar colors can be used. As a result, it becomes difficult to discern the signature.

Fig. 5 shows an example in which a special pattern is displayed on the background. For example, as shown in Fig. 5, a hatched pattern is displayed on the background, and hence it becomes difficult to discern the signature data 103. The special pattern is not necessarily a hatched pattern. Any image pattern can be used as long as the signature is difficult to discern.

Fig. 6 shows an example in which the signature data 103 is partially displayed. For example, the signature data 103 is displayed in dotted lines instead of solid lines.

Alternatively, only portions near the beginning point and the end point of a stroke can be displayed, thereby making it difficult to discern the signature data 103.

Fig. 7 shows an example in which a displayed signature is successively deleted immediately after the signature data 103 is displayed. For example, it is assumed that the coordinates of the input signature data 103 are displayed for a period of 0.1 second. If the entire signature data 103 is written in 2 seconds, approximately 1/20th of the entirety is displayed at any given time. The signature data 103 can be obtained not only as shape information but also as information indicating writing timing and time interval. Dynamic display of the signature data 103 is very important in assisting the user to remember his/her signature. Referring to Fig. 7, the signature is displayed as it is input. In addition, the signature is deleted a very short period of time after it is input. As a result, it becomes difficult to discern the signature.

Fig. 8 is a flowchart showing a scrambling process illustrated in Fig. 7. The inputting of a signature starts in step S801. In step S802, the process displays the currently-input coordinates (signature data 103) of a currently-input stroke. In step S803, the process deletes displayed coordinate data (signature data 103) which is input a predetermined period of time previously, e.g., 0.1

second previously. The deletion is performed by re-rendering the stroke which had been input a short time previously in the current display loop using rendering XOR.

Alternatively, only one stroke (part of the entire signature) which is currently being input may be displayed.

Fig. 9 shows an example in which the signature data 103 is flashed when it is being displayed. When the signature is input, the state in which the signature is displayed and the state in which the signature is deleted are switched every predetermined period of time. As a result, it becomes difficult to discern the signature data 103.

Fig. 10 is a flowchart showing the scrambling process illustrated in Fig. 9. For example, two logical graphics screens are retained. On one logical screen (first logical screen), a stroke (input coordinates) is rendered. On the other screen (second logical screen), white is displayed. In the rendering loop, only one of the logical screens is displayed. A timer measures a predetermined period of time, and when it is time to change the display, the currently-displayed logical screen is changed to the other logical display screen. The inputting of a signature starts in step S1001. In step S1002, the process renders coordinates which are input on the first logical screen. While the first logical screen is displayed, the signature being input is displayed. While the second logical screen is displayed, a

white screen is displayed. In step S1003, the process determines whether it is time to change the displayed screen. If the determination is affirmative, the process changes the displayed logical screen in step S1004.

As described above, according to the embodiment of the present invention, it is possible to prevent others from discerning a signature being input by displaying the signature as in Figs. 4 to 10.

A combination of the display scrambling methods performed in the display scrambling step 109, which are described with reference to Figs. 4 to 10, can be used.

In this embodiment, as shown in Fig. 3, the displaying of the signature at the time the signature is registered is described. However, the display scrambling step 109 is not limited to this embodiment. The display scrambling step 109 can be applied to cases in which the signature is authenticated, re-registered, or re-displayed. As a result, it is possible to prevent others from discerning the signature.

According to this embodiment, handwritten data can be displayed so that it is difficult to be discerned by others while allowing the user who has written the data to recognize the data to a certain degree. Thus, the security of the authentication system is enhanced.

If a user forgets signature data registered by the user,

display is performed to enable only the user to remember the forgotten signature data. As a result, the user can recall the registered signature to mind.

The implementation of all of the elements and steps described above is within the ordinary level of skill in the relevant technical field, using components and techniques that are commercially available and/or well known to those in the art.

While the present invention has been described with reference to what are presently considered to be the preferred embodiments, it is to be understood that the invention is not limited to the disclosed embodiments. On the contrary, the invention is intended to cover various modifications and equivalent arrangements included within the spirit and scope of the appended claims. The scope of the following claims is to be accorded the broadest interpretation so as to encompass all such modifications and equivalent structures and functions.